DOCID: 4165174

~~TOP SECRET//COMINT//NOFORN~~
NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

02 March 2010

MEMORANDUM FOR THE ASSISTANT TO THE SECRETARY OF DEFENSE (INTELLIGENCE OVERSIGHT)

SUBJECT: (U//~~FOUO~~) Required Actions for the CY 2009 Intelligence Oversight Report to Congress – INFORMATION MEMORANDUM

(U//~~FOUO~~) In accordance with your memorandum of 21 October 2009, the enclosed consolidation of the National Security Agency's Quarterly Reports to the President's Intelligence Oversight Board for calendar year 2009 is provided to assist the Secretary of Defense in preparation of his Annual Report to Congress.

George Elland

GEORGE ELLARD
Inspector General

Encl:
Annual Report

This document may be declassified and marked "UNCLASSIFIED//FOR ~~OFFICIAL USE ONLY~~" upon removal of enclosure(s).

Approved for Release by NSA on 12-19-2014, FOIA Case # 70809 (Litigation)

DOCID: 4165174

1. (U//~~FOUO~~) Intelligence, counterintelligence, and intelligence-related activities that violate law, regulation, or policy substantiated during the year, as well as actions taken as a result of the violations

(b)(1)
(b)(3)-P.L. 86-36

(U) Intelligence Activities

(U) Unintentional Collection against United States Persons or Persons in the United States

~~(TS//SI//NF)~~ [redacted] instances in which Signals Intelligence (SIGINT) analysts inadvertently collected communications to, from, or about United States (U.S.) persons while pursuing foreign intelligence tasking were reported in CY 2009. Those instances of unintentional collection were caused by tasking selectors (e.g., telephone numbers) thought to be foreign that were discovered to be in the United States, delays in detasking, procedural errors, software-related problems, typographical errors, one case in which Communications Security (COMSEC) monitoring data was inappropriately reviewed, and other human error. Intercepts and reports have been deleted or destroyed where required by United States SIGINT Directive (USSID) SP0018.

~~(TS//SI//REL TO USA, FVEY)~~ During this reporting period, [redacted] valid foreign intelligence targets [redacted] the United States. Collection on those targets occurred due to detasking delays, software-related problems, procedural errors, and human error.

(U) Tasking Error

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//REL TO USA, FVEY)~~ A U.S. telephone number was mistakenly tasked for collection. [redacted] an NSA analyst tasked a telephone number believed to be associated with a foreign intelligence target. [redacted] The selector was detasked on [redacted] and one resulting intercept was deleted. No reports were issued on the collection.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//REL TO USA, FVEY)~~ [redacted] an NSA [redacted] learned that tasked telephone number selectors believed to be used by foreign intelligence targets [redacted] The resulting collection of [redacted] calls was deleted and the selectors were detasked on [redacted] No reporting was produced based on the collection.

(U) One End of the Communication in the United States

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ By agreement, pursuant to Executive Order (E.O.) 12333, unminimized SIGINT [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

Derived From: NSA/CSSM 1-52
Dated: 20070108
Declassify On: 20320108

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(U) Poorly Constructed Database Queries

~~(TS//SI//NF)~~ On occasions, NSA analysts employed poorly constructed database queries, and on of those occasions, the queries returned results from the database. Problems were caused by analysts querying selectors thought to be foreign but were discovered to be in the United States, misunderstandings of authority, overly broad search terms, procedural errors such as failure to confirm the location of targets, software-related problems, other human error, and one case in which COMSEC selectors were used in a SIGINT database. The returned results from the overly broad or incomplete queries were deleted, and no reports were issued. NSA counseled or retrained analysts who misunderstood NSA authorities.

(U) Detasking Delays

(b)(1)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) On occasions, NSA analysts failed to remove selectors from tasking due to human and procedural errors.

(U//~~FOUO~~) Dissemination of U.S. Identities

~~(TS//SI//REL TO USA, FVEY)~~ The NSA enterprise issued approximately SIGINT product reports during 2009. In those reports, there were instances in which SIGINT analysts disseminated communications to, from, or about U.S. persons while pursuing foreign intelligence. A total of SIGINT products were cancelled as NSA analysts learned of the U.S. persons, organizations, or entities named in the products without authorization. The data was deleted or destroyed when required and the reports were not reissued or they were reissued with proper minimization.

(U) Report Cancellation Delay

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ an NSA analyst learned from that a valid foreign target held dual and U.S. citizenship. Although the selectors were detasked on and collection was purged from NSA databases, reports generated from the unauthorized collection were not cancelled until The delay in report cancellation occurred because of a miscommunication between two analysts. Each believed the other was going to cancel the reports.

~~(TS//SI//REL)~~ a SIGINT analyst forwarded an e-mail containing a U.S. identity without considering USSID SP0018 implications. The e-mail was recalled, and the customer was asked to destroy copies of the information.

(U) Foreign Intelligence Surveillance Act (FISA) Activities

~~(TS//SI//NF)~~ NSA incurred violations related to Foreign Intelligence Surveillance Court (FISC)-authorized targets in 2009. There were instances in which selectors were detasked

(b)(1)
(b)(3)-P.L. 86-36

late, [redacted] in which tasking occurred before authorization, [redacted] in which selectors [redacted] instances of misunderstanding the authority, [redacted] in which FISC-approved selectors were misused, [redacted] from an unapproved selector, and [redacted] from other human error. There was also one case of improper dissemination.

(b)(1)
(b)(3)-P.L. 86-36

(U) Retention

~~(S//REL TO USA, FVEY)~~ [redacted] an NSA database developer noted that a database contained FISA data older than the retention time authorized by the Court. All files containing the FISA data were moved [redacted] To prevent future retention errors, the developers implemented a process [redacted] containing FISA data.

~~(TS//SI//NF)~~ [redacted]

-P.L. 86-36
-18 USC 798
-50 USC 3024(i)

~~(TS//SI//NF)~~ Business Records FISA (BR FISA)

~~(TS//SI//NF)~~ There were two violations of the BR FISC Order, one due to lack of Reasonable Articulable Suspicion (RAS) and one for exceeding call chaining guidelines. No data was retained, and no reports were issued. Additionally, an NSA analyst forwarded reports to personnel who did not have required BR Order training.

~~(TS//SI//NF)~~ [redacted] the Department of Justice reported to the FISC that the NSA had been using an "alert list" to compare incoming BR FISA metadata against telephone numbers associated with counterterrorism (CT) targets that the NSA had tasked for SIGINT collection. The alert list contained numbers that NSA determined that a RAS existed and that the numbers were related to a terrorist organization associated with [redacted] However, the majority of selectors on the alert list had not been subjected to a RAS determination. Analysis through call-chaining was not performed unless the number met the RAS standard.

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ [redacted] the NSA suspended the comparison of BR FISA metadata against CT target selectors, and during a comprehensive review, the NSA identified other processes used to query the BR FISA metadata that also did not conform with the Court's orders or that were not fully explained to the Court. The review also identified some manually entered queries that were noncompliant with the Court's orders. None of the compliance incidents resulted in the dissemination of any reporting from the NSA to any other department or agency. Upon discovery of these compliance incidents, the NSA immediately made changes to its processes to ensure that handling and querying of the telephony metadata was in accordance with the Court's orders. The corrective measures included implementation of controls to prevent any automated querying of the telephony

metadata NSA receives pursuant to the Court's orders and to guard against manual querying errors.

~~(TS//SI//NF)~~ The Department of Justice filed preliminary notices of compliance incidents with the FISC on 15 January, 21 January, 26 January, 2 February, 25 February, and 31 March 2009. The FISC issued an order on 5 March 2009 that allowed NSA to continue to acquire the BR FISA metadata but imposed further restrictions on use of the data.

~~(TS//SI//NF)~~ On 24 June 2009, during the end-to-end review of the FISA BR Order implementation, the review team found that NSA disseminated one SIGINT product report in a manner not authorized by the FISA BR Order. The report, containing U.S. information, [redacted] purged the data from its repositories on 24 June 2009.

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(TS//SI//NF)~~ Pen Register/Trap and Trace Order (PR/TT)

~~(TS//SI//NF)~~ There were two violations of the PR/TT Order due to an analyst using an earlier version of a software tool [redacted] and a new software tool that [redacted]

~~(TS//SI//NF)~~ In Court Order PR/TT [redacted] and previous orders, the FISC authorized the installation and use of pen registers and trap and trace devices as described in the government's application to collect specific information likely to identify the sources or destinations of specified electronic communications [redacted] NSA's Office of General Counsel learned that [redacted] not specifically authorized by the Order. [redacted] NSA informed the Department of Justice's National Security Division that, in consultation with the Director, NSA/Chief, CSS, it had instructed NSA analysts to cease querying the PR/TT metadata until the matter was resolved and with the Court's express approval to resume receipt of specified communications and to resume its previous operational practices. The Order expired [redacted] Data in NSA's possession was quarantined and collection ceased.

(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ **The Protect America Act of 2007 (PAA)** There were [redacted] PAA incidents in 2009 due to tasking selectors thought to be foreign but discovered to be in the United States, delays in detasking, tasking selectors under the wrong certification, and a typographical error.

(U) The FISA Amendments Act (FAA)

(b)(1)
(b)(3)-P.L. 86-36

(U) Section 702

~~(TS//SI//NF)~~ There were [redacted] violations of FAA Section 702 authority due to tasking under the wrong FAA certification, [redacted] violations due to tasking selectors thought to be foreign but discovered to be in the United States, [redacted] violations due to detasking delays, [redacted] violations due to software errors, [redacted] violations where no reasonable articulable suspicion was found, one

violation due to collection at an unapproved location, one violation due to procedural error, and one violation for tasking prior to approval.

(U) Dissemination of FAA Data

~~(TS//SI//NF)~~ unminimized collection containing a U.S. selector was forwarded to in an analyst-to-analyst exchange. When the violation was identified, the message was successfully recalled

(U//~~FOUO~~) an NSA analyst forwarded FAA data to NSA personnel, some of whom were not authorized to view FAA data. The e-mail was recalled and recipients deleted copies on

(b)(1)
(b)(3)-P.L. 86-36

(U//~~FOUO~~) an NSA analyst forwarded an e-mail containing FAA data to recipients, three of whom had not completed training required for access to FAA information. Within one hour of recognizing the mistake, the three analysts not authorized access to FAA data had deleted the e-mail.

~~(TS//SI//NF)~~ On occasions in November 2009, NSA analysts forwarded unminimized FAA SIGINT on targets tasked under FAA customer not authorized to view unminimized FAA SIGINT. In the instances, e-mail selectors associated with U.S. entities or persons were left unminimized in SIGINT reporting. All reports were either revised or reissued with proper minimization.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) Destruction Delay

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ U.S. person data was retained before an NSA analyst purged it from NSA databases. The target, believed to be foreign at the time of tasking on was found to be a U.S. citizen in The analyst intended to request authorization to retain the calls collected but did not pursue the request. The collection was purged from NSA databases No reports were issued.

(U) Section 704

~~(TS//SI//NF)~~ There were violations of FAA Section 704 due to delays in detasking selectors when the targets were discovered to be in the United States, one violation for incorrect date ranges, and one violation for tasking a selector belonging to a U.S. person.

(U) Section 705b

(b)(1)
(b)(3)-P.L. 86-36

~~(TS//SI//NF)~~ There were violations of FAA Section 705b due to detasking delays, one violation due to querying a selector when the target was in the United States, violations due to miscellaneous human error, one violation due to failure to follow procedure, one violation due to querying more data than authorized, one violation due to an unauthorized selector, and violations due to delays in purging data.

~~(TS//SI//NF)~~ in response to a request from senior managers, an NSA analyst queried a raw SIGINT database using selectors associated with a U.S. person not authorized for collection under FAA. The analyst conducted the search because The analyst also believed that The analyst was before a U.S. person is targeted. The query produced no results and no reports were issued.

(b)(1)
(b)(3)-P.L. 86-36

(U) **Other**

(U) Unauthorized Access to SIGINT

~~(S//REL TO USA, FVEY)~~ There were incidents of unauthorized access to SIGINT, including FISA, FAA, and PAA data, due to procedural errors, sharing of accounts, human error, and lack of training.

(U) Improper Storage of SIGINT Data

~~(S//REL TO USA, FVEY)~~ There were incidents of improper storage of SIGINT data, to include improperly labeled FISA data, U.S. identities entered into a database, and human error.

(U) Dissemination

~~(S//REL TO USA, AUS, GBR, NZL)~~ NSA terminated (b)(1)
)-P.L. 86-36
)-50 USC 3024(i)
While researching the problem, NSA recognized and rectified weaknesses with additional oversight and internal controls related to filtering, training analysts, and reviewing audit trails.

(b)(1)
(b)(3)-P.L. 86-36

~~(C//NF)~~ data that was not releasable to e-mails were deleted upon recognition.

~~(S//SI//REL TO USA, FVEY)~~ By agreement, SIGINT intercept is forwarded, notified NSA and destroyed the intercept. As a result of these instances, formal procedures for handling U.S. person information are being developed for these

~~(TS//SI//NF)~~ **Computer Network Exploitation (CNE)**

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

[redacted]

~~(TS//SI//NF)~~ [redacted]

(U) Intelligence-related Activities

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(S//SI//NF)~~ To reduce the risk of unauthorized telephony collection and prevent violations, NSA instituted a process that gives analysts greater and faster insight into a target's location [redacted] when collection occurred, it was purged from NSA's principal raw SIGINT repositories when required.

~~(TS//SI//NF)~~ Similarly, [redacted] NSA analysts found that [redacted] e-mail selectors [redacted] Collection that occurred in [redacted] of the [redacted] instances was purged from NSA databases when required.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U//~~FOUO~~) Although not violations of E.O. 12333 and related directives, the NSA reports 30 instances in which database access was not terminated when it was no longer required. Once identified, the accesses were terminated.

~~(TS//SI//NF)~~ Additionally, there were [redacted] violations resulting from collection on U.S. persons as follows: [redacted] due to a [redacted] with data collected; [redacted] due to failure to perform an origin check prior to tasking [redacted] due to [redacted] accessing a database containing data [redacted] and [redacted] due to [redacted] sharing.

(b)(1)
(b)(3)-P.L. 86-36

2. (U) NSA OIG Intelligence Oversight Inspections, Investigations, and Special Studies

(U) Queries not Reviewed

(U//~~FOUO~~) Due to a lack of trained personnel at a SIGINT site, [redacted] individuals were not reviewing audit trails of raw SIGINT queries. [redacted] that account was subsequently suspended. NSA was not able to determine the volume of queries not reviewed [redacted]. The site is arranging additional training for all site audit trail reviewers.

(b)(1)
(b)(3)-P.L. 86-36

(U) Intelligence Oversight Inspections

(U) NSA/CSS Threat Operations Center (NTOC)

(U//~~FOUO~~) An NSA OIG inspection found that the intelligence oversight within NTOC is appropriately managed and compliant with regulations. NTOC has established effective management controls to ensure that [redacted] authorities are properly executed on the NTOC operations floor. Based on training statistics reviewed, the inspection found a 95 percent rate of compliance for intelligence oversight training.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(U) NSA/CSS Texas (NSAT)

(U//~~FOUO~~) Joint IG inspectors examined intelligence oversight (IO) program management, IO training, IO knowledge, and the application of IO. Despite fragmented oversight of IO training, NSAT operates well in the application of NSA authorities. The recently appointed IO program manager is well known and has begun to make improvements to the site's IO processes. The governing mission directive does not encompass responsibilities for the oversight of reservists working NSAT missions or delineate Service Cryptologic Component (SCC) responsibilities. A highlight of the inspection was the meticulous tracking of sensitive SIGINT database accesses within several mission product lines.

(U//~~FOUO~~) Investigation of Alleged Improprieties at NSA Georgia (NSAG)

(b)(3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ On 14 August 2009, the NSA OIG completed an investigation into an allegation that the [redacted] program at NSAG unlawfully intercepted and processed U.S. person communications. [redacted] Our investigation included four interviews of the complainant, more than [redacted] witness interviews, [redacted] and the forensic analysis of almost [redacted] records. We found no targeting of U.S. persons by [redacted]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

(U//~~FOUO~~)

(U//~~FOUO~~) Additionally, the NSA OIG substantiated an allegation that an NSAG analyst, had queried a raw SIGINT database on a selector of a person in the United States. The person was a relative of a valid foreign intelligence target.

(U//~~FOUO~~) **Alleged Unauthorized Disclosure of Classified Information and Misuse of the United States SIGINT System (USSS)**

~~(S//SI//REL TO USA, FVEY)~~ a soldier in a U.S. Army used the USSS to target his wife, who was also a soldier stationed He queried an NSA database for her Following questions from his auditor, the soldier confessed his actions. After investigation by the unit substantiated the misuse, the soldier received nonjudicial punishment. Through a Uniformed Code of Military Justice (UCMJ) Field Grade Article 15, the soldier's rank was reduced from Sergeant to Specialist, he was given 45 days extra duty, and he was required to forfeit one half month's pay for two months (suspended for 180 days). In addition, the unit has revoked the soldier's access to classified information.

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI//REL TO USA, FVEY)~~ an Army analyst assigned to the reportedly queried in violation of USSID SP0018. According to the analyst, he queried the foreign numbers to aid in learning the language. The analyst's action was not in support of his official, mission-related duties. The analyst's database access and his access to classified information have been suspended.

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

DOCID: 4165174